hb

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,010	02/27/2002	Chi Hung Tong	009661-0029-999	4019

7590 05/17/2005

CHARLES E. MILLER
DICKSTEIN SHAPIRO MORIN & OSHINSKY LLP
1177 AVENUE OF THE AMERICAS
41ST FLOOR
NEW YORK, NY 10036-2714

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/087,010	**Applicant(s)** TONG ET AL.	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2002* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *2/27/2002*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Detail Action

1. Claims 1-18 are presented for examination.

Drawings

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Gehrmann et al. (Gehrmann, Patent No.: US 6,779,111 B1).

As per claim 1, Gehrmann teaches a communication system for communicating securely encrypted messages, comprising:

i. a resource-constrained client (col. 4 lines 63-65, and fig. 3 No. 310);

ii. a gateway server possessing high computational power capable of doing fast and dynamic encryption-related computations when requested by the client and returning the result to the client (col. 3 lines 11-17, and fig. 3 No. 320);

iii. an application server communicating encrypted messages with the client (col. 5 lines 13-15, and fig. 3 No. 330); and

iv. a communication network connecting the client, the gateway server, and the application server (col. 4 lines 40-49).

As per claim 2, Gehrmann teaches the communication system, wherein the communication network is a wireless communication network (col. 4 lines 40-49).

As per claims 3, Gehrmann teaches the communication method, wherein the gateway server is a wireless gateway server (col. 4 lines 40-49).

As per claim 4, Gehrmann teaches the method, wherein the client is a mobile device (col. 4 lines 62-65).

As per claim 5, Gehrmann teaches the communication system, wherein the encrypted messages are encoded using public-key cryptography (col. 3 lines 51-67).

As per claim 6, Gehrmann teaches the communication system, wherein the public-key cryptography is achieved using RSA algorithm (col. 3 lines 51-67).

As per claim 7, Gehrmann teaches the communication system, wherein the client further comprises means for storing and generating the encryption key, generating random numbers and doing modular multiplication (fig. 4 No. 402 & 404, and col. 6 lines 8-15).

As per claim 8, Gehrmann teaches the communication system, wherein the random numbers are generated for scrambling the encryption key and the original message as well as decomposing the encryption key (fig. 4 No. 404, and col. 6 lines 8-15).

As per claim 9, Gehrmann teaches the communication system, wherein the scrambled and decomposed encryption key and the scrambled original message are sent from the client to the gateway server (fig. 4 No. 406, and col. 6 lines 25-37).

As per claim 10, Gehrmann teaches the communication system, wherein the modular multiplication is performed based on the result returned by the gateway server (col. 6 lines 52-57, and col. 7 lines 5-21).

As per claim 11, Gehrmann teaches the communication system, wherein the encryption-related computations performed by the gateway server are integer exponentiation (col. 3 lines 11-16, and col. 6 lines 25-37).

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 12, and 15-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Kawamura et al. (Kawamura, Patent Number: 5,369,708).

As per claims 12, and 15, Kawamura teaches a two-iteration client-server encryption method for protecting encrypted messages from attacks made by un-trusted server, comprising the steps of:

i. the client generates multiple sets of random numbers (fig. 8 step ST51);

ii. the client uses each set of random numbers to scramble both the encryption key and the original message as well as decompose the encryption key (col. 4 lines 47-col. 5 lines 3, and fig. 8 step ST52);

iii. the client sends each set of scrambled and decomposed encryption key and the scrambled message to the server (fig. 8 step ST54);

iv. the server computes the exponentiation of each set of the scrambled message being raised to the power of each decomposed scrambled encryption key in the same set (fig. 8 steps ST55-ST57, and col. 10 lines 15-22);

v. the server sends the computation results to the client (fig. 8 step ST57);

vi. the client extracts the encrypted message for each set using a modular multiplication of the results returned by the sever (col. 10 lines 23-32, and fig. 8 steps S58 & ST59);

vii. the client feeds the encrypted messages once more to the server and the server performs the exponentiation one more time (col. 10 lines 37-42, and fig. 9 steps ST61-ST64); and

viii. the client derives the encrypted messages one more time and verifies if each set returns the same encrypted message (col. 10 lines 44-56, and fig. 10 step ST63).

As per claim 16, Kawamura teaches the method, wherein the number of sets of random numbers is three (fig. 6 step ST31, and col. 8 lines 49-50).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 13-14 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al. (Kawamura, Patent Number: 5,369,708) further in view of Gehrmann et al. (Gehrmann, Patent No.: US 6,779,111 B1)

As per claims 13, and 17, Kawamura teaches all the subject matter as described above.

Kawamura does not explicitly disclose a mobile device like PDA and mobile phone. Kawamura however suggests his invention is not limited to a mobile device IC card and the communication line alone. He teaches, besides his invention, modifications may be made without departing from the novel and advantageous features of his invention (Kawamura col. 4 lines 23-24 and col. 14 lines 21-31).

However Gehrmann teaches the method, wherein the client is a mobile device (col. 4 lines 62-65).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention was made to employ the teachings of Gehrmann within the system of Kawamura because it would enable having low computing power such as mobile phones or PDAs to have faster response times by using the higher computing power of an untrusted proxy while still keeping end-to-end security (Gehrmann col. 7 lines 5-10).

As per claims 14, and 18, Kawamura teaches all the subject matter as described above.

Kawamura does not explicitly disclose a wireless gateway server. Kawamura however suggests his invention is not limited to a mobile device IC card and the communication line alone. Kawamura teaches, besides his invention, modifications may be made without departing from the novel and advantageous features of his invention (Kawamura col. 4 lines 23-24 and col. 14 lines 21-31).

However Gehrmann teaches the communication system/method, wherein the gateway server is a wireless gateway server (col. 4 lines 40-49).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention was made to employ the teachings of Gehrmann within the system of Kawamura because it would enable having low computing power such as mobile phones or PDAs to have faster response times by using the higher computing power of an untrusted proxy while still keeping end-to-end security (Gehrmann col. 7 lines 5-10).

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
May 12, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100